Secure Services Gateway (SSG)

Maintenance Guide

in support of the Secure Access and Control Offer (SAC) R3.0

19-300174
Issue 6
August 2005

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this Documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s): Designated System(s) License (DS).

End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Shrinkwrap License (SR)

With respect to Software that contains elements provided by third party suppliers, End user may install and use the Software in accordance with the terms and conditions of the "shrinkwrap" or "clickwrap" license accompanying the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Copyright" below for more information).

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's web site at:
http://support.avaya.com/LicenseInfo/

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

For additional support telephone numbers, see the Avaya Web site:
http://www.avaya.com/support

Trademarks

Avaya is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Document ordering information:

Avaya Publications Center

Voice:	+1-207-866-6701
	1-800-457-1764 (Toll-free, U.S. and Canada only)
Fax:	+1-207-626-7269
	1-800-457-1764 (Toll-free, U.S. and Canada only)
Write:	Globalware Solutions
	200 Ward Hill Avenue
	Haverhill, MA 01835 USA
	Attention: Avaya Account Manager
Web:	http://www.avaya.com/support
Email:	totalware@gwsmail.com
Order:	Document No. 19-300174, Issue 6.0
	August 2005

For the most current versions of documentation, go to the Avaya support Web site:
http://www.avaya.com/support

Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is 1 800 242 2121 in the United States. For additional support telephone numbers, see the Avaya Web site:
http://www.avaya.com/support

Contents

Chapter 1: Maintenance Overview 5
Chapter contents 5
Overview 5
Related resources 6
Linux operating system manuals 8

Chapter 2: Hardware Upgrade and Maintenance 9
In this chapter 9
Installation guidelines 9
System reliability guidelines 10
Handling static sensitive devices 10
General safety guidelines 11
Replacing the hard drive 12
Tasks to replace the hard drive 13
Replacing the hard drive in an x305 IBM server 14
Replacing the hard drive in an x306 IBM server 18
Replacing the x305 IBM server's RSA 19
Replacing the server's dual NIC 20

Chapter 3: Server Initialization and Shutdown 21
Chapter contents 21
Server initialization 21
System shutdown 22

Chapter 4: Operating System Monitoring 23
Chapter contents 23
Gathering system information 23
Monitoring system processes 23
Memory usage 24
File systems 25
Additional resources 26

Chapter 5: Operating System Recovery 27
Chapter contents 27
Hardware/software problems 27
Root password 27
Booting into rescue mode 28

Booting into single-user mode 30
Booting into emergency mode 31

Chapter 6: SSG Configuration Backup and Restore 33
Chapter contents 33
Backing up the SSG configuration 33
Restoring the SSG configuration 36

Index 37

Chapter 1: Maintenance Overview

Chapter contents

This chapter contains the following sections:

- Overview
- Related resources
- Linux operating system manuals

Overview

The Secure Access and Control Offer Basic and Premium Offers allow secure remote servicing of customer devices by means of the Internet Protocol (IP). SAC traffic between the customer's and Avaya's infrastructure is via a Virtual Private Network (VPN) or Frame Relay. SAC uses the Red Hat® Enterprise Linux® Standard 3.0 operating system on the Secure Services Gateway (SSG) component.

This manual provides information on administration and maintenance of the Secure Services Gateway (SSG) hardware and operating system. This includes the following:

- Replacing hardware components.
- Monitoring the operating system. See Operating System Monitoring on page 23.
- Performing an operating system recovery. See Operating System Recovery on page 27.
- Perform a backup or restore of the Secure Services Gateway (SSG) Configuration. See SSG Configuration Backup and Restore on page 33.

Related resources

You can download the following documents at http://support.avaya.com/sac.

Table 1: Related Resources

Document Title	Document No.	Content
SSG and NIU Installation and Configuration	19-300173	Procedures for hardware and software installation and configuration. Description of IBM hardware x305 and x306 servers. Also contains information on customer vs. Avaya responsibilities like VPN, upgrades, updates, and so forth.
SSG Quick Setup Guide	19-300175	A summary of steps to successfully get the SSG (both hardware and software) up and running properly.
NIU Quick Setup Guide: For non-preloaded, non-Avaya-labeled, Lantronix products	19-300246	A summary of steps to successfully get the NIU (both hardware and software) up and running properly. This Quick Setup Guide is for non-preloaded, non-Avaya labeled Lantronix NIUs.
NIU Quick Setup Guide: For preloaded firmware and preconfigured NIUs	19-300552	A summary of steps to successfully get the NIU (both hardware and software) up and running properly. This Quick Setup Guide is for Lantronix NIUs that have preloaded firmware and are preconfigured for Avaya.
SSG User Guide	19-300393	Provides step-by-step instructions to configure and maintain the SSG Web interface, as well as, a description of each field in the Web interface.
Job Aid: Configuration of G3si Release 6 through 9 Including Release 9.5 or higher, If the CLAN Board Is NOT Installed for SAC Offer Support	19-300247	Describes the steps required to configure a G3si r6-r9, or higher, if no CLAN is installed for support of the SAC offer.
Job Aid: Configuration of INTUITY AUDIX R4.x for SAC Offer Support	19-300276	Provides the required steps for Tier 3 Support to configure INTUITY AUDIX Release 4.x for support of the SAC offer

1 of 2

Table 1: Related Resources (continued)

Document Title	Document No.	Content
Job Aid: Configuration of INTUITY AUDIX R5.1.46 for SAC Offer Support	19-300277	Describes the steps required for Craft Level Support to configure an INTUITY AUDIX Release 5.1.46 for support of the SAC offer.
Job Aid: Configuration of IR1.2/1.2.1 for SAC Offer Support	19-300254	Describes how to configure Interactive Response (IR) version 1.2 or 1.2.1 for support by the SAC offer.
Job Aid: Configuration of S8xxx Media Servers for SAC Offer Support	19-300255	Describes how to configure an s8710, s8700, s8500 and s8300 Media Server for support of the SAC offer.
Job Aid: Configuration of CMS v9 or v11 for SAC Offer Support	19-300397	Describes how to configure Call Management System (CMS) version 11 or for support by the SAC offer.
Job Aid: G3r Configuration Release 6 through 9, Including Release 9.5 or Higher, If the CLAN Board Is NOT Installed for SAC Offer Support	19-300398	Describes how to configure a G3r release 6 through 9 or higher, including release 9.5 or higher, if no CLAN board is installed, for support by the SAC offer.
Job Aid: Restoring the Avaya Default Settings on the NIU	19-300551	Describes how to restore Avaya's default settings on a Network Interface Unit (NIU) used for the SAC offer.
Job Aid: Installing RedHat Enterprise Linux AS on the SSG Server	19-300559	Describes how to install Linux AS and the SSG software on the SSG server.
Job Aid: Configuring Modular Messaging to forward alarms to the SSG	19-300644	Describes how to configure Modular Messaging (MM) for support by the SAC offer.
Job Aid: Configuring MAPD for SAC Offer Support	19-300645	Describes how to configure the Multi-Application Platform for Definity (MAPD) for support by the SAC offer.
Job Aid: Installing and configuring a non-preloaded, non-Avaya labeled Lantronix NIU	19-300646	Describes how to install, configure, and test a non-preloaded, non-Avaya labeled Lantronix NIU. This job aid is for Lantronix NIUs that do not have preloaded firmware and have not been preconfigured for Avaya.
		2 of 2

Linux operating system manuals

For detailed information on the Red Hat Enterprise Linux Standard 3.0 operating system, Avaya recommends that you see the Red Hat web site to download manuals you may need.

To obtain the appropriate manuals, do the following:

1. In a browser, type: www.redhat.com
2. Click **Support** on the home page.
3. Under the column **Support Resources**, go to **Documentation**.
4. From the drop-down menu, select **Red Hat Enterprise Linux**. A list of manuals appears.

Chapter 2: Hardware Upgrade and Maintenance

In this chapter

This chapter describes how to maintain and replace various hardware components of the SSG server. This chapter contains the following sections:

- Installation guidelines
- Removing the cover of the x305 IBM server
- Replacing the hard drive
- Replacing the x305 IBM server's RSA
- Replacing the server's dual NIC

Important:

Before performing the procedures in this chapter, Avaya recommends that you back up the SSG configuration to a server in your LAN.For details on backing up the server, see Backing up the SSG configuration on page 33.

Installation guidelines

Before you begin installing options on your server, remember the following:

- Make sure that you have an adequate number of properly grounded electrical outlets for your server, monitor, and other devices that you will connect to the server.
- Back up all important data before you make changes to disk drives.
- Have a small Phillips screwdriver and small flat-blade screwdriver available.
- For a list of supported options for your server, see http://support.avaya.com .

System reliability guidelines

To help ensure proper system cooling and system reliability, make sure that:

- Each of the drive bays has a drive or a filler panel.
- Space is available around the server to allow the server cooling system to work properly. See the documentation that comes with the rack.
- You have followed the cabling instructions that come with optional adapters.
- You replace a failed fan as soon as possible.

Handling static sensitive devices

CAUTION:
Static electricity can damage electronic devices, including your server. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them.

To reduce the possibility of damage from electrostatic discharge, observe the following precautions:

- Limit your movement prior to doing any maintenance. Movement can cause static electricity to build up around you.
- Handle all devices carefully, holding each device by its edge or its frame.
- Do not touch solder joints, pins, or exposed circuitry.
- Do not leave the device where others can handle and damage it.
- While the device is still in its static-protective package, touch it to an unpainted metal part of the server for at least 2 seconds. This drains static electricity from the package and from your body.
- Remove the device from its package and install it directly into the server without setting down the device. If it is necessary to set down the device, place it back into its static-protective package. Do not place the device on your server cover or on a metal surface.
- Take additional care when handling devices during cold weather since that is when static electricity is at its greatest threat. Heating reduces indoor humidity and increases static electricity.

General safety guidelines

Follow these rules to ensure general safety:

- Observe good housekeeping in the area of the machines during and after maintenance.
- When lifting any heavy object:
  1. Ensure you can stand safely without slipping.
  2. Distribute the weight of the object equally between your feet.
  3. Use a slow lifting force. Never move suddenly or twist when you attempt to lift.
  4. Lift by standing or by pushing up with your leg muscles; this action removes the strain from the muscles in your back. *Do not attempt to lift any objects that weigh more than 16 kg (35 lb.) or objects that you think are too heavy for you.*
- Do not perform any action that causes hazards to yourself or those around you, or that makes the equipment unsafe.
- Before you start the machine, ensure that other service representatives and the customer's personnel are not in a hazardous position.
- Place removed covers and other parts in a safe place, away from all personnel, while you are servicing the machine.
- Keep your tool case away from walk areas so that other people will not trip over it.
- Do not wear loose clothing that can be trapped in the moving parts of a machine. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.
- Insert the ends of your necktie or scarf inside clothing or fasten it with a nonconductive clip, approximately 8 centimeters (3 inches) from the end.
- Do not wear jewelry, chains, metal-frame eyeglasses, or metal fasteners for your clothing.

  Note:

  Metal objects are good electrical conductors.
- Wear safety glasses when you are: hammering, drilling soldering, cutting wire, attaching springs, using solvents, or working in any other conditions that might be hazardous to your eyes.
- After service, reinstall all safety shields, guards, labels, and ground wires. Replace any safety device that is worn or defective.
- Reinstall all covers correctly before returning the machine to the customer.

Replacing the hard drive

The server comes with one integrated drive electronics (IDE) CD-ROM drive, one 1.44 MB diskette drive, and a hard disk drive.

This section contains the following topics:

- Tasks to replace the hard drive. This section provides a table that outlines the tasks involved in replacing the hard drive in an x305 or x306 server.
- Replacing the hard drive in an x305 IBM server
- Replacing the hard drive in an x306 IBM server

CAUTION:

Wear an antistatic wrist ground strap whenever handling components such as the hard drive of an IBM server. Connect the strap to an approved ground, such as an unpainted metal surface. Also, place the hard drive on an antistatic mat that is similarly grounded. Do not place the new or the old drive on a bare surface.

Important:

If the hard drive *is* functional, before performing the following procedure, back up the SSG configuration to a server on the LAN. For details on backing up the server, see Backing up the SSG configuration on page 33.

If the hard drive is *not* functional, make sure the customer has a recent backup of SSG configuration that you can restore after you have replaced the hard drive. If not, after replacing the hard drive, you must reconfigure the server as if it were a new installation. For information on how to perform initial configuration, see *SSG and NIU Installation and Configuration*, document number 19-300173. You can download this document at http://support.avaya.com/sac.

Tasks to replace the hard drive

Table 2 outlines the tasks involved in replacing the hard drive of an x305 or x306 IBM server.

Table 2: Tasks for replacing the hard drive in an x305 or x306 IBM server

✓		Task	Description
	1	Shut down the server.	• If the hard drive is functional, enter the **shutdown -h now** command. The internal fan shuts off. For more information, see System shutdown on page 22. • If the hard drive is not functional, press the power-control button to power down the server. **CAUTION:** Do not hold down the power button for more than a split second. Holding the button down too long causes the server to reboot.
	2	Unplug the server.	Once the server is completely shut down (the green power-on LED is blinking), unplug the power cord from the server. Disconnect and label the LAN connections from the Ethernet ports on the RSA and dual NIC (if used). Disconnect all attached devices, including the laptop, and the external flashcard reader (if used).
	3	Make server top accessible.	Pull the server forward until the mounting rails lock into place. **Note:** You do not need to remove the server from the rails.
	4	Replace the hard drive.	• **x305**: see Replacing the hard drive in an x305 IBM server. • **x306**: see Replacing the hard drive in an x306 IBM server.
	5	Slide the server back in place.	Release the retaining tabs on the rails and slide the server back into place in the data rack.

1 of 2

Table 2: Tasks for replacing the hard drive in an x305 or x306 IBM server (continued)

✓		Task	Description
	6	Power up the server	Plug the power cords into the server and RSA. Press the power-control button on the front of the server. **Note:** Wait at least 3 minutes for the server to complete its power up. Watch the power-on LED on the server (the green LED is on steady).
	7	Reconnect attached devices	Reconnect all attached devices, including the laptop and the external flashcard reader (if used).
			2 of 2

Replacing the hard drive in an x305 IBM server

This procedure consists of the following steps:

1. Removing the cover of the x305 IBM server
2. Removing the hard drive from the x305 IBM server
3. Installing the new hard drive in the x305 IBM server
4. Replacing the cover of the x305 IBM server

Removing the cover of the x305 IBM server

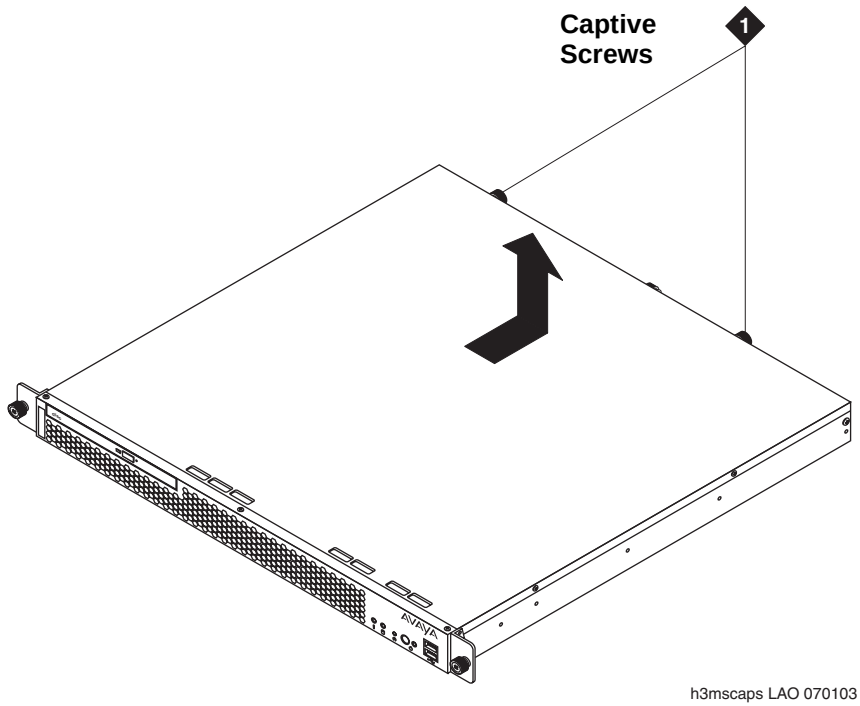
To remove the server cover:

Note:

Read General safety guidelines and Handling static sensitive devices.

1. With the server extended on the slide rails, loosen the 2 captive screws on the back of the server that hold the top in place. See Figure 1.

Figure 1: Captive screws on cover



2. Slide the server cover back from the front panel until the cover's tabs are released from the top slot of the front panel.
3. Lift the cover straight up and remove it from the server.

CAUTION:

For proper cooling and air flow, place the cover back on the server before turning the power on. Operating the server for extended periods of time (over 30 minutes) with the cover removed might damage server components.

Removing the hard drive from the x305 IBM server

To remove the hard drive from the server:

1. Locate the drive cage in the left-hand corner of the front of the server. See Figure 2.

Figure 2: Removing and replacing the drive cage

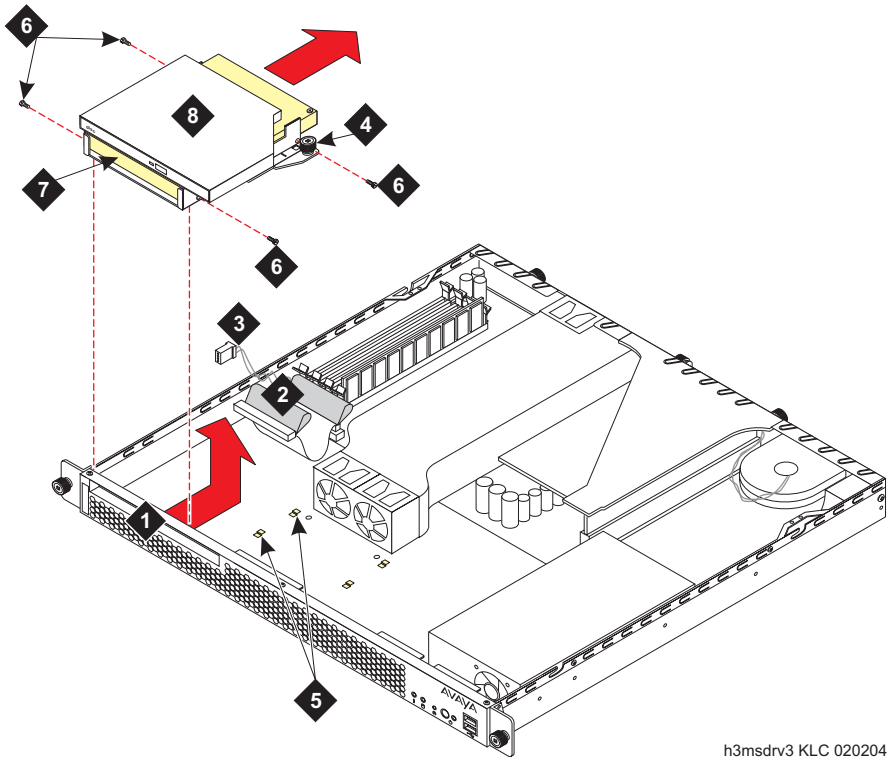


Figure notes:

1.	Drive bay housing drive cage	**5.**	Tabs
2.	Ribbon cable attached to hard drive	**6.**	Screws holding hard drive in drive cage
3.	Cable connected to the CD-ROM drive	**7.**	Hard drive
4.	Captive screw holding drive cage	**8.**	Drive cage

2. Use the black pull handles on the ribbon cables to unplug the data connectors from the back of the CD-ROM drive and hard drive.
3. Push the ribbon cable back out of the way.

4. Unplug the two power connectors from the back of the CD-ROM drive and the hard drive. You must release the power connector on the CD-ROM drive by gently bending the side spring clip holding it in place.
5. Loosen the captive screw next to the drive cage.
6. Slide the drive cage toward the back of the server to clear the retaining hooks.
7. Place the drive cage on the antistatic mat.
8. Remove the four screws (two on each side) securing the hard drive in the drive cage and remove the hard drive.

Installing the new hard drive in the x305 IBM server

To install the new hard drive in the server:

1. Insert the new hard drive into the drive cage so that the connectors are in the same direction as the CD-ROM connectors and the screw holes are aligned. See Figure 2: Removing and replacing the drive cage on page 16.
2. Reinsert the 4 screws (2 on each side) to attach the hard drive to the drive cage.
3. Reattach the flat ribbon cable (in 2 places) to the hard drive and CD-ROM drive.
4. Reattach the 2 power cables to the hard drive and CD-ROM drive.
5. Slide the drive cage into place in the server, making sure that it fits securely into the four retaining hooks and finger-tighten the captive screw.
6. Make sure the drive cage is secure and that the cables are not bunched or blocking the fan unit.

Replacing the cover of the x305 IBM server

To replace the cover of the server:

1. Place the cover onto the server.
2. Slide the cover forward so the cover's tabs slide into place under the top slots of the front panel.
3. Finger-tighten the captive screws on the back of the server. See Figure 1: Captive screws on cover on page 15.

Replacing the hard drive in an x306 IBM server

This procedure consists of the following steps:

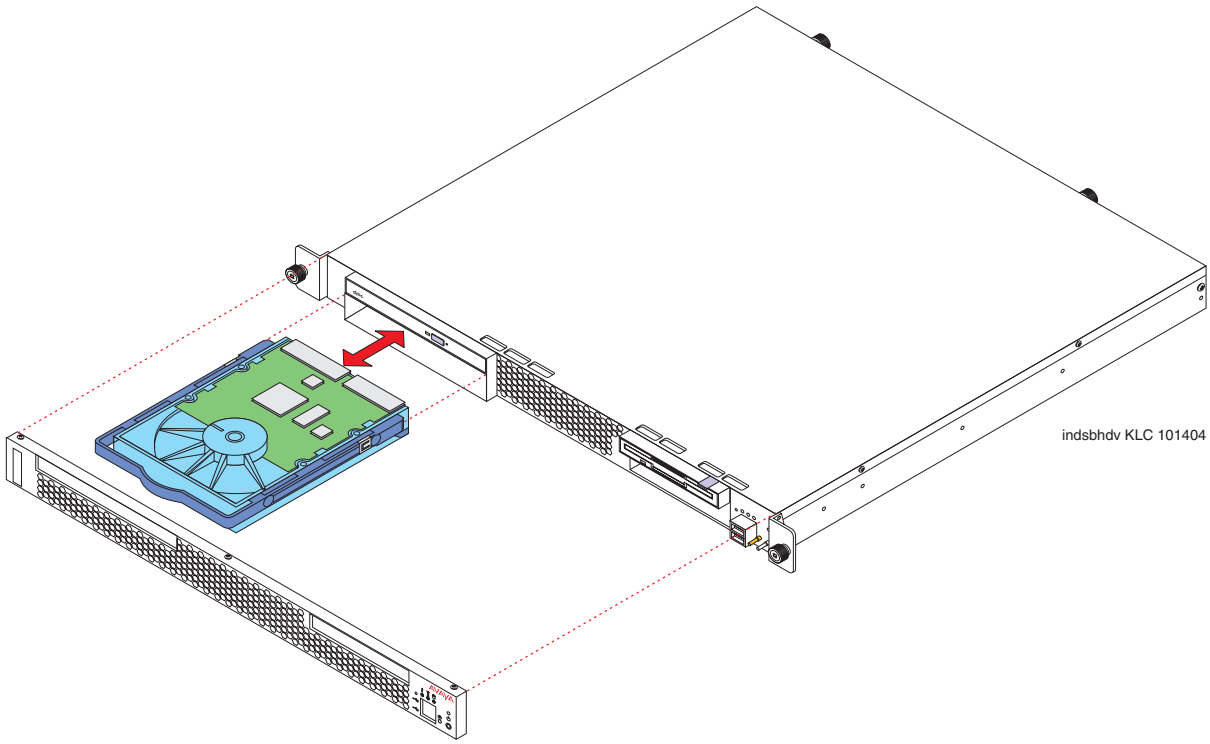
1. Removing the hard drive from the x306 IBM server
2. Installing the new hard drive in the x306 IBM server

Removing the hard drive from the x306 IBM server

To remove the hard drive from the server:

1. Press the release tabs on the bezel and pull the bezel away from the server. See Figure 3.

Figure 3: Removing and installing the hard drive



2. Pull the hard drive from the server.
3. To remove the hard drive from the drive tray, unscrew the four screws and remove the hard drive.

Installing the new hard drive in the x306 IBM server

To install the new hard drive:

1. Position the hard drive on the drive tray and secure with the four screws.
2. Slide the hard drive into the server (see Figure 3: Removing and installing the hard drive on page 18).
3. Reinstall the bezel.

Replacing the x305 IBM server's RSA

For information on how to replace the x305 IBM server's RSA, see *Job Aids for Field Replacements: Avaya S8500 Media Servers*, document number 03-300529.

To download this document, see http://support.avaya.com. You can search for the document by its document number, 03-300529.

Note:

The S8500 and the x305 IBM server are the same server. S8500 is the Avaya-branded Communication Manager server.

Note:

When replacing the SSG server's RSA, back up the SSG configuration for Step 2. This step of the job aid, backing up the media server, is not applicable for the SSG server.

Replacing the server’s dual NIC

For information on how to replace the x305 or x306 IBM server’s dual network interface card (NIC), see *Job Aids for Field Replacements: Avaya S8500 Media Servers*, document number 03-300529.

To download this document, see http://support.avaya.com. You can search for the document by its document number, 03-300529.

Note:

The S8500 and the x305 IBM server are the same server. And the S8500B and the x306 IBM server are the same server. S8500 and S8500B are the Avaya-branded Communication Manager servers.

Note:

When replacing the SSG server’s dual NIC, back up the SSG configuration for Step 1. This step of the job aid, backing up the media server, is not applicable for the SSG server.

Chapter 3: Server Initialization and Shutdown

Chapter contents

This chapter describes various maintenance aspects of servers and their troubleshooting, including:

- Server initialization
- System shutdown

Server initialization

After a server is powered on, software/firmware modules are executed in the following order:

1. **BIOS** — The BIOS (Basic Input/Output System) takes control of the server's CPU and provides several services including:
   - Running diagnostics on the server's hardware (processor, memory, disk, etc.).
   - Reading the 512-byte master boot record (MBR) from the boot sector of the boot disk into memory and passing control to it. The MBR contains phase 1 of the Linux loader (LILO).
2. **LILO** — The Linux loader (LILO) reads the Linux kernel from the boot disk and transfers control to it. Phase 1 of LILO was read into memory by the BIOS. When Phase 1 begins executing, it reads in the rest of the LILO program, including the Linux kernel's location. LILO reads in the Linux kernel, uncompresses it, and transfers control to it.
3. **Linux Kernel** — The Linux kernel initializes the CPU's registers, initializes its own data structures, determines the amount of available memory, initializes the various compiled-in device drivers, etc. When finished, the Linux kernel creates the first process, known as *init*.
4. **Init** — The *init* process creates the remaining processes for the system using the **/etc/inittab** file, which specifies runlevels, and a set of processes to run at each runlevel. During this step, the SSG application and database are started.

   The rc script runs the service startup scripts in **/etc/rc.d/rc4.d** in numeric order (S00* through S99*). Each of these startup scripts starts a particular Linux service (e.g., inetd). In addition to starting up the various services, the disk partitions are checked for sanity, and loadable modules are loaded.

   Note:

   Use the Linux command **statapp** to view the status of the applications.

System shutdown

Use the **shutdown** command to shut down the system.

To shut down the system, the root user may issue the **/sbin/shutdown** command. The shutdown main page has a complete list of options, but the two most common uses are:

- shutdown -h now
- shutdown -r now

After shutting everything down, the **-h** option halts the machine, and the **-r** option reboots.

Chapter 4: Operating System Monitoring

Chapter contents

This section describes how to monitor the various operating system functions. This includes:

- Gathering system information
- Monitoring system processes
- Additional resources

Gathering system information

Before configuring your operating system, you gather essential system information using simple Linux commands and programs. For example, you should know

- how to find the amount of free memory,
- the amount of available hard drive space,
- how your hard drive is partitioned, and
- what processes are running.

Monitoring system processes

The **ps ax** command displays a list of current system processes. To display the process owner along with the processes, use the command **ps aux**. This list is a static list; in other words, it is a snapshot of what is running when you invoked the command. If you want a constantly updated list of running processes, use **top** as described below.

The **ps** output can be long. To prevent it from scrolling off the screen, you can pipe it through less:

ps aux | less

You can use the **ps** command in combination with the **grep** command to see if a process is running. For example, to determine if **Emacs** is running, use the following command:

ps ax | grep emacs

The **top** command displays currently running processes and important information about the process, including their memory and CPU usage. The list is both real-time and interactive.

To exit **top**, press the **q** key.

Useful interactive commands that you can use with **top** include the following:

Table 3: Interactive Commands

Command	Description
[Space]	Immediately refresh the display
[h]	Display a help screen
[k]	Kill a process. You will be prompted for the process ID and the signal to send to it.
[n]	Change the number of processes displayed. You will be prompted to enter the number.
[u]	Sort by user
[M]	Sort by memory usage
[P]	Sort by CPU usage

Memory usage

The **free** command displays the total amount of physical memory and swap space for the system as well as the amount of memory that is used, free, shared, in kernel buffers, and cached.

```
               total          used      free      shared    buffers       cached
Mem:           256812         240668    16144     105176    50520         81848
-/+ buffers/cache:            108300    148512
Swap:          265032         780264252
The command free -m shows the same information in megabytes, which are easier to read.
               total          used      free      shared    buffers       cached
Mem:           250            235       15        102       49            79
-/+ buffers/cache:            105       145
Swap:          258              0       258
```

File systems

The **df** command reports the systems' disk space usage. If you type the command df at a shell prompt, the output looks similar to the following:

```
Filesystem     1k-blocks     Used       Available     Use%    Mounted on
/dev/hda2      10325716      2902060    6899140       30%     /
/dev/hda1      15554         8656       6095          59%     /boot
/dev/hda3      20722644      2664256    17005732      14%     /home
none           256796        0          256796        0%      /dev/shm
```

By default, this utility shows the partition size in 1 kilobyte blocks and the amount of used and available disk space in kilobytes. To view the information in megabytes and gigabytes, use the command **df -h**.

The **-h** argument stands for human-readable format. The output looks similar to the following:

```
Filesystem            Size   Used     Avail    Use%    Mounted on
/dev/hda2             9.8G   2.8G     6.5G     30%     /
/dev/hda1             15M    8.5M     5.9M     59%     /boot
/dev/hda3             20G    2.6G     16G      14%     /home
none                  251M   0        250M     0%      /dev/shm
```

Virtual memory

In the list of partitions, there is an entry for **/dev/shm**. This entry represents the systems' virtual memory file system.

Space used by files in a directory

The **du** command displays the estimated amount of space being used by files in a directory. If you type **du** at a shell prompt, the disk usage for each of the subdirectories will be displayed in a list. The total for the current directory and subdirectories will also be shown as the last line in the list. If you do not want to see the totals for all the subdirectories, use the command **du -hs** to see only the total for the directory in human-readable format. Use the **du --help** command to see more options.

42.4. Hardware

You can also use the **lspci** command to list all PCI devices. Use the command

- **lspci -v** for detailed information or
- **lspci -vv** for detailed information plus additional output.

For example, **lspci** can be used to determine the manufacturer, model, and memory size of a system's video card:

01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04) \ (prog-if 00 [VGA])

Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max Flags: medium devsel, IRQ 16

Memory at f4000000 (32-bit, prefetchable) [size=32M]

Memory at fcffc000 (32-bit, non-prefetchable) [size=16K] Memory at fc000000 (32-bit, non-prefetchable) [size=8M]

Expansion ROM at 80000000 [disabled] [size=64K] Capabilities: [dc] Power Management version 2 Capabilities: [f0] AGP version 2.0

Note:

You can use the **lspci** command to determine the network card in your system if you do not know the manufacturer or model number.

Additional resources

To learn more about gathering system information, see the following resources:

- Using commands:
  - **ps --help** — Displays a list of options that can be used with **ps**.
  - **top** manual page — Type **man top** to learn more about **top** and its many options.
  - **free** manual page — type **man free** to learn more about **free** and its many options.
  - **df** manual page — Type **man df** to learn more about the **df** command and its many options.
  - **du** manual page — Type **man du** to learn more about the **du** command and its many options.
  - **lspci** manual page — Type **man lspci** to learn more about the **lspci** command and its many options.
  - **/proc/ directory** — The contents of the **/proc/** directory can also be used to gather more detailed system information. Refer to the Red Hat Enterprise Linux Reference Guide for additional information about the **/proc/** directory.
- Linux Manuals:
  - Go to the Red Hat Enterprise Linux web site for the manuals.
    1. In a browser, type: www.redhat.com
    2. Click **Support** on the home page.
    3. Under the column **Support Resources**, go to **Documentation**.
    4. From the drop-down menu, select **Red Hat Enterprise Linux**. A list of manuals appears.

Chapter 5: Operating System Recovery

Chapter contents

This chapter describes how to recover from problems with the Red Hat Enterprise Linux Server Edition 3.0 operating system. The topics included in this section are:

- Hardware/software problems
- Booting into single-user mode
- Booting into emergency mode

Hardware/software problems

This category can result from a variety of issue. Examples of this type of problem include:

- failing hard drives, or
- specifying an invalid root device or kernel in the boot loader configuration file.

If these problems occur, you may not be able to reboot the Red Hat Enterprise Linux. You can use one of the system recovery modes to try and resolve the problem, or, get copies of the most important files.

Root password

If you forget your root password, do the following:

1. Boot into rescue mode or single-user mode. See Booting into rescue mode.
2. Use the **passwd** command to reset the root password.

Booting into rescue mode

Rescue mode provides the ability to boot a small Red Hat Enterprise Linux environment entirely from a diskette, CD-ROM, or some other boot method instead of the system's hard drive.

During normal operation, the Red Hat Enterprise Linux Server Edition 3.0 system uses files located on the system’s hard drive to do all functions, including run programs and store files. However, if you cannot access files on the system’s hard drive, you can use rescue mode to access the files stored on the system’s hard drive. This is done even if you cannot run Red Hat Enterprise Linux from the hard drive. Use the following procedure to boot into rescue mode:

1. In order to boot into rescue mode, you must be able to use one of the following methods:
   - Using an installation boot diskette.
   - Using an installation boot CD-ROM.
   - Using the Red Hat Enterprise Linux CD-ROM #1.
2. Add the keyword **rescue** as a kernel parameter. For example, for an x86 system, type the following command at the installation boot prompt:

   linux rescue
3. Answer the prompts, including which language to use. It also prompts you to select where a valid rescue image is located. Select from **Local CD-ROM**, **Hard Drive**, **NFS image**, **FTP**, or **HTTP**. The location selected must contain a valid installation tree, and the installation tree must be for the same version of Red Hat Enterprise Linux as the Red Hat Enterprise Linux CD ROM #1 from which you booted.

   Note:

   If you used a boot CD-ROM or diskette to start rescue mode, the installation tree must be from the same tree from which the media was created. For more information about how to setup an installation tree on a hard drive, NFS server, FTP server, or HTTP server, see the *Red Hat Enterprise Linux Installation Guide*.
4. If you select a rescue image that does not require a network connect, you are asked whether or not you want to establish a network connection. A network connection is useful if you need to backup files to a different computer or install some RPM packages from a shared network location, for example. You will also see the following message:

```
The rescue environment will now attempt to find your Red Hat
Linux installation and mount it under the directory
/mnt/sysimage. You can then make any changes required to your
system. If you want to proceed with this step choose
'Continue'. You can also choose to mount your file systems
read-only instead of read-write by choosing 'Read-only'.
If for some reason this process fails you can choose 'Skip'
and this step will be skipped and you will go directly to a
command shell.
```

5. Depending on you selection, the following occurs
   - If you select **Continue**, the system attempts to mount your file system under the directory **/mnt/sysimage/**. If it fails to mount a partition, it notifies you.
   - If you select **Read-Only**, the system attempts to mount your file system under the directory **/mnt/sysimage/**, but in read-only mode.
   - If you select **Skip**, the file system is not mounted. Choose **Skip** if you think your file system is corrupted.
6. Once the system is in rescue mode, a prompt appears on virtual console 1 and virtual console 2 (use the **Ctrl**+**Alt**+**F1** key combination to access virtual console 1 and **Ctrl**+**Alt**+**F2** to access virtual console 2):

   sh-2.05b#

   - If you selected **Continue** to mount your partitions automatically and they were mounted successfully, you are in single-user mode.

     Even if your file system is mounted, the default root partition while in rescue mode is a temporary root partition, not the root partition of the file system used during normal user mode (runlevel 3 or 5). If you selected to mount your file system and it mounted successfully, you can change the root partition of the rescue mode environment to the root partition of your file system by executing the following command:

     chroot /mnt/sysimage

     This is useful if you need to run commands such as **rpm** that require your root partition to be mounted as **/**. To exit the chroot environment, type **exit**, and you will return to the prompt.
   - If you selected **Skip**, you can try to mount a partition manually inside rescue mode by creating a directory such as */foo*, and typing the following command:

     mount -t ext3 /dev/hda5 /foo

     In the above command, */foo* is a directory that you have created and */dev/hda5* is the partition you want to mount. If the partition is of type **ext2**, replace **ext3** with **ext2**. If you do not know the names of your partitions, use the following command to list them:

     fdisk -l (one)

     From the prompt, you can run many useful commands such as
     - **list-harddrives** to list the hard drives in the system
     - **ssh**, **scp**, and **ping** if the network is started
     - **parted** and **fdisk** for managing partitions
     - **rpm** for installing or upgrading software
     - **joe** for editing configuration files (If you try to start other popular editors such as **emacs**, **pico**, or **vi**, the **joe** editor will be started.)

Booting into single-user mode

The advantage of single-user mode is that you do not need a boot diskette or CD-ROM. However, it does not give you the option to

- mount the file systems as read-only or
- not mount them at all.

If your system boots, but does not allow you to log in when it has completed booting, try single-user

mode. In single-user mode, your computer boots to runlevel 1. Your local file systems are mounted, but your network is not activated. You have a usable system maintenance shell. Unlike rescue mode, single-user mode automatically tries to mount your file system.

CAUTION:

Do not use single-user mode if your file system cannot be mounted successfully. You cannot use single-user mode if the runlevel 1 configuration on your system is corrupted.

On an x305 IBM Server system using GRUB as the boot loader, use the following steps to boot into single-user mode:

1. If you have a GRUB password configured, type **p** and enter the password.
2. Select **Red Hat Enterprise Linux** with the version of the kernel that you wish to boot and type **a** to append the line.
3. Go to the end of the line and type **single** as a separate word. Press [Enter] to exit edit mode.

   Tip:

   Press the [Spacebar] and then type **single**.
4. Back at the GRUB screen, type **b** to boot into single-user mode.
   - On an x305 IBM Server system using LILO as the boot loader, at the LILO boot prompt, type: **linux single**

   Note:

   If you are using the graphical LILO, press **Ctrl-x** to exit the graphical screen and go to the `boot:` prompt.
   - For all other platforms, specify **single** as a kernel parameter at the boot prompt.

Booting into emergency mode

In emergency mode, you are booted into the most minimal environment. The root file system is mounted read-only and the setup is minimal.

The advantage of emergency mode over single-user mode is that the **init** files are not loaded. If **init** is corrupted or not working, you can still mount file systems to recover data that could be lost during a reinstallation.

To boot into emergency mode, use the same method as described for single-user mode in Booting into single-user mode.

On an x305 IBM Server system using GRUB as the boot loader, use the following steps to boot into emergency mode:

1. If you have a GRUB password configured, type **p** and enter the password.
2. Select **Red Hat Enterprise Linux** with the version of the kernel that you wish to boot and type **a** to append the line.
3. Go to the end of the line and type **emergency** as a separate word. Press [Enter] to exit edit mode.

   Tip:

   Press the [Spacebar] and then type **emergency**.
4. Back at the GRUB screen, type **b** to boot into single-user mode.
   - On an x305 IBM Server system using LILO as the boot loader, at the LILO boot prompt, type: **linux single**

   Note:

   If you are using the graphical LILO, press **Ctrl-x** to exit the graphical screen and go to the `boot:` prompt.
   - For all other platforms, specify **emergency** as a kernel parameter at the boot prompt.

Chapter 6: SSG Configuration Backup and Restore

Chapter contents

This section describes how to backup and restore the Secure Services Gateway (SSG) configuration:

- Backing up the SSG configuration
- Restoring the SSG configuration

Backing up the SSG configuration

Avaya recommends that you create a backup copy of configuration information after configuring SSG, and continue to do backups on a routine basis. The backup process creates a **gzip** compressed tar file containing all configuration and log files. The name of the backup file is: **SSG-Backup-<date-time>.tgz**, where *<date-time>* is the date and time the backup occurred. The Product ID, a 10-digit number used to identify each Avaya device on your network, is included in the backup filename only if it is configured during installation. In this case, the backup filename is of the form: **SSG-<*Product Id*>-Backup-<*date-time*>.tgz**.

The backup file is stored on the SSG and can be backed up by any backup management system for the host. In addition (or if the local host is not backed up), you can opt to copy the backup file to a remote host when you configure the backup process.

Important:

If you configure the backup process to copy the backup data to a remote host, the upload link to the host must be able to sustain 10 kbps.

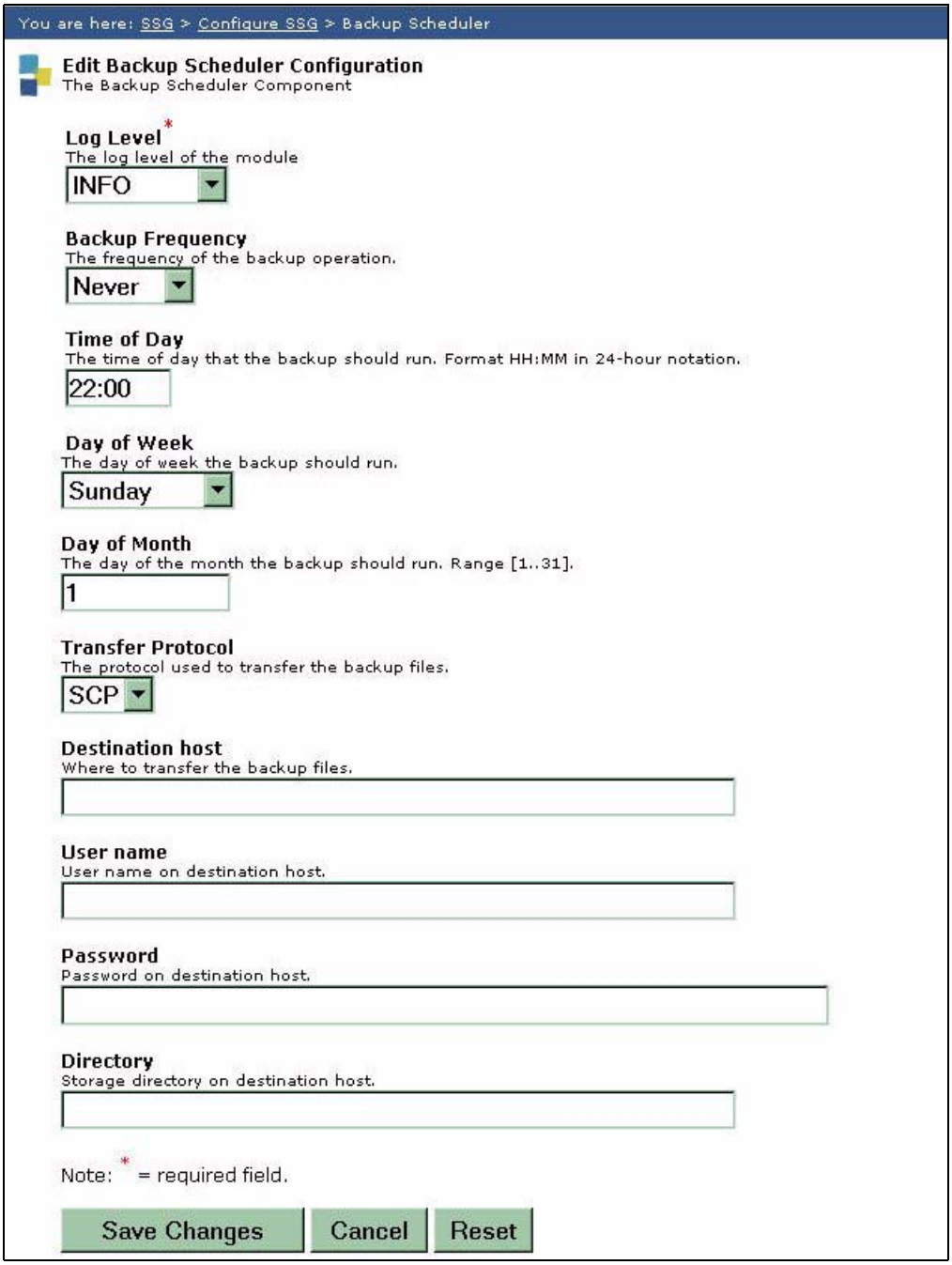
Tip:

The status of each backup is logged in the SSG log. To confirm that backups are completed successfully, check the log regularly. Successful backups are logged as informational messages, and backup errors are logged as warnings.

To backup configuration data:

1. From the Main Menu, click **Configure SSG**. The SSG Configuration page displays.
2. In the Actions column of the Backup Scheduler row, click **Edit**. The Edit Backup Scheduler Configuration page displays. See Figure 4.

Figure 4: Edit Backup Scheduler Configuration Page



3. In the **Log Level** list box, click the message severity level that you want logged for this software module. Messages of the severity you select and of all higher severities are logged. For example, if you select **Information**, messages of severity levels Information, Warning, and Severe are logged.

4. In the **Backup Frequency** list box, click the frequency of the backup operation. Options are never, daily, weekly, or monthly.

   Note:

   The frequency you select in the Backup Frequency list box maps to the relevant field below. For example, if you select **Monthly**, then the Day of Month field applies. In this instance, the Time of Day and Day of Week fields are ignored.

   - In the **Time of Day** field, type the time (in 24 hour format) of the backups. Use this field only when you select **Daily** in the Backup Frequency field.
   - In the **Day of Week** list box, click the weekday of the backups. Use this field only when you select **Weekly** in the **Backup Frequency** field.
   - In the **Day of Month** field, type the calendar day (as a number). Use this field only when you select **Monthly** in the **Backup Frequency** field.

5. If you want to upload the backup data to a remote host, enter the appropriate information in the following fields. If you leave these fields blank, the backup file is not copied to a remote host.

   a. In the **Transfer Protocol** list box, select the protocol used to transfer the backup data. Options are Secure Copy Program (SCP) or File Transfer Protocol (FTP).

      - If SCP is used, you need to run an SSH daemon on the destination host.
      - If FTP is used, you need to run an FTP daemon on the destination host.

   Note:

   For backup by FTP, the standard port is used.

   b. In the **Destination host** field, type the DNS name or IP address of the host to upload the data to for the backup operation.

   c. In the **User name** field, type the user name of the destination host. The user name is a user account on the destination host that has permissions to write to the destination directory.

   d. In the **Password** field, type the password of the destination host. This is the password for the user account in step 8c.

   e. In the **Directory** field, type the full path of the storage directory of the backup files.

6. Click **Save Changes**.

   Note:

   SSG backup data contains the product id and date and time. If the same host performs a backup within a minute (60 seconds), the backup data will be overwritten.

Restoring the SSG configuration

To restore the SSG configuration:

1. Log onto the machine as the **avadmin** user
2. Copy the backup file to the home directory of **avadmin**.
3. Stop the SSG software by entering the following command:

   ssg.sh stop
4. Unzip the backup file to a temporary directory. For example:
   a. **mkdir tempdir**
   b. **cd tempdir**
   c. **tar zfx ~/SSG-<Product Id>-<Date-Time>.tgz**
5. Remove the current contents of the SSG Data directory by entering the following command:

   rm -fr ~/SSG/Data/*
6. Move the backup data to the SSG Data directory:

   mv Backup/* ~/SSG/Data
   a. To restore the database, you must do the following steps. Type:

      cd ~/SSG/Data/db
   b. Type:

      gunzip dbdump-2004-05-07.tgz

   Note:

   The date in the example above should be changed based on the date the backup was performed.

   - This command will expand the file to the filename **dbdump-2004-05-07.tar**

   c. Type:

      sudo /etc/init.d/avdb start
   d. Type:

      pg_restore -v -p 6543 -d avssgdb -a -Ft --no-owner <dbdumpfile_name>.tar

   Note:

   The restore can take several minutes to complete. Large restores can take several hours.
7. Restart the SSG software to load the backed up configuration. Type the following command:

   ssg.sh start

Index

B

basic input/output system, see BIOS
BIOS 21

I

initialization
  and recovery 21
  init process 21
  server 21

L

Linux
  commands
    statapp 21
  kernel 21
  loader 21
  scripts
    rc 21
    service startup 21

M

master boot record (MBR) 21

R

rc Linux script 21

S

servers
  initialization 21
  software/firmware modules 21
startup Linux scripts 21
statapp Linux command 21
status
  Linux commands
    statapp command 21